420 Rec'd PCT/PTO 29 SEP 1999

FORM PTO-1390 REV. 5-93	US DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEYS DOCKET NUMBER P99,1784
TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371		U.S.APPLICATION NO. (if known, see 37 CFR 1.5) 09/402144
INTERNATIONAL APPLICATION NO. **PCT/DE98/00563**	INTERNATIONAL FILING DATE **25 February 1998**	PRIORITY DATE CLAIMED **14 April 1997**

TITLE OF INVENTION

"METHOD AND SYSTEM FOR PRODUCING AND CHECKING A HASH TOTAL FOR DIGITAL DATA GROUPED IN SEVERAL DATA SEGMENTS"

APPLICANT(S) FOR DO/EO/US

MARTINA HANCK, ET AL.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay.
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. ☒ A copy of International Application as filed (35 U.S.C. 371(c)(2)) - drawings attached.
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2) - drawings attached.

7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. §371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.

8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).

9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. ☒ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98; **(PTO 1449, Prior Art, Search Report)**.

12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included. **(SEE ATTACHED ENVELOPE)**

13. ☒ Amendment "A" Prior to Action.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.

14. ☐ A substitute specification.

15. ☐ A change of power of attorney and/or address letter.

16. ☒ Other items or information:
    a. ☒ Submission of Drawings - 1 sheet of drawings, single figure; and
    Request for Approval of Drawing Additions, 1 sheet of drawings, single figure.

    b. ☒ EXPRESS MAIL #EL378698319US dated September 29, 1999.

420 Rec'd PCT/PTO 29 SEP 1999

U.S. APPLICATION NO (if known, see 37 C.F.R. 1.5)	INTERNATIONAL APPLICATION NO	ATTORNEY'S DOCKET NUMBER
09/402144	PCT/DE98/00563	P99,1784

17. ☒ The following fees are submitted:

	CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 C.F.R. 1.492(a)(1)-(5):		
Search Report has been prepared by the EPO or JPO $840.00		
International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) $670.00		
No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but international search fee paid to USPTO (37 C.F.R. 1.445(a)(2) $760.00		
Neither international preliminary examination fee (37 C.F.R. 1.482) nor international search fee (37 C.F.R. 1.445(a)(2) paid to USPTO $970.00		
International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) . . . . . $ 96.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 840.00	
harge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months the earliest claimed priority date (37 C.F.R. 1.492(e)).	$	

ms	Number Filed		Number Extra	Rate		
al Claims	36	- 20 =	16	X $ 18.00	$ 288.00	
pendent Claims	06	- 3 =	03	X $ 78.00	$ 234.00	
tiple Dependent Claims				$260.00 +	$	
TOTAL OF ABOVE CALCULATIONS =					$ 1362.00	
iction by ½ for filing by small entity, if applicable. Verified Small Entity statement must be filed. (Note 37 C.F.R. 1.9, 1.27, 1.28)					$	
SUBTOTAL =					$ 1362.00	
essing fee of $130.00 for furnishing the English translation later than ☐ 20 ☐ 30 hs from the earliest claimed priority date (37 CFR 1.492(f)). +					$	
TOTAL NATIONAL FEE =					$ 1362.00	
Fee for recording the enclosed assignment (37 C.F.R. 1.21(h). The assignment must be accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). $40.00 per property +						
TOTAL FEES ENCLOSED =					$ 1362.00	
					Amount to be refunded	$
					charged	$

a. ☒ A check in the amount of $ 1362.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. **08-2290**. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Hill & Simpson
A Professional Corporation
85th Floor Sears Tower
Chicago, Illinois 60606

Steven H. Noll
SIGNATURE

Steven H. Noll
NAME

28,982
Registration Number

BOX PCT

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

APPLICANT(S):	Martina Hanck, et al
ATTORNEY DOCKET NO.:	P99,1784
INTERNATIONAL APPLICATION NO:	PCT/DE98/00563
INTERNATIONAL FILING DATE:	25 February 1998
INVENTION:	"METHOD AND SYSTEM FOR PRODUCING AND CHECKING A HASH TOTAL FOR DIGITAL DATA GROUPED IN SEVERAL DATA SEGMENTS"

Assistant Commissioner for Patents,
Washington D.C. 20231

AMENDMENT "A" PRIOR TO ACTION

Sir:

Applicants herewith amend the above-referenced PCT application, and request entry of the Amendment prior to examination on the United States Examination Phase.

IN THE SPECIFICATION:

On page 1, cancel lines 2-6, and substitute the following therefor:

--SPECIFICATION

TITLE

METHOD AND SYSTEM FOR PRODUCING AND CHECKING A HASH TOTAL FOR DIGITAL DATA GROUPED IN SEVERAL DATA SEGMENTS

BACKGROUND OF THE INVENTION

Field of the invention–;

in line 8, after "i.e.", insert --,--;

in line 10, cancel "protect the" and substitute --protect various aspects-- therefor, and cancel "with respect to the most varied aspects";

in line 12, cancel "A" and substitute --One-- therefor;

in line 13, after "the", insert --integrity of--;

in line 14, cancel "the so-called protection of the integrity of the data";

above line 16, insert

--**Description of the Related Art**--;

in line 17, cancel "the so-called" and substitute --a-- therefor;

in line 18, cancel ", for example" and substitute --such as-- therefor;

in line 19, cancel "[1]" and substitute --W. Stallings, Sicherheit in Netzwerk und Internet (Security in Network and Internet), Prentice Hall, ISBN 3-930436-29-9, pp. 203-223, 1995 (Stallings)-- therefor;

in line 20, cancel "[1]"and substitute --Stallings-- therefor;

in line 22, cancel "means" and substitute --way-- therefor;

in line 24, after "integrity", insert --of the data--;

in line 29, cancel "are matched" and substitute --match-- therefor;

in line 31, cancel "previously" and substitute --known-- therefor;

in line 32, cancel "necessitates that" and substitute --requires-- therefor, and cancel "must" and substitute --to-- therefor;

in line 35, cancel "since otherwise" and substitute --; if it is not,-- therefor;

in line 36, cancel "errored" and substitute --erroneous-- therefor; and

in line 39, after "segments", insert --,--.

On page 2, in line 2, cancel "or it is not" and substitute --; it may not be-- therefor;

in line 3, cancel "In the" and substitute --The-- therefor;

in line 4, cancel "from [1], it is therefore required for" and substitute --

described in Stallings requires-- therefor;

in line 6, cancel "that is to say";

in line 10, cancel "expenditure and substitute --overhead-- therefor;

in line 11, after "is", insert --even--;

in line 14, cancel "From [2], commutative" and substitute --Commutative-- therefor, and after "known", insert --from K. H. Kiyek and F. Schwarz, Mathmatik für Informatiker (Mathematics for Computer Scientists), Teubner Verlag, ISBN 3-519-03277-X, pp. 11-13, 1989 (Kiyek & Schwarz)--, and cancel "In [2]," and substitute --Kiyek & Schwarz include" therefor;

in line 15, cancel "is also specified. Illustratively, a commutative operation" and substitute --which-- therefor;

in line 18, cancel "each order" and substitute --any ordering-- therefor;

in line 19, cancel "operation" and substitute --operations-- therefor;

in line 21, cancel "EXOR" and substitute --exclusive OR (EXOR)-- therefor;

in line 23, cancel "From [3], a" and substitute --A-- therefor;

in line 26, after "known", insert --from German patent DE-A 2 048 365--;

above line 27, insert

--**SUMMARY OF THE INVENTION**--;

cancel lines 33-36, and substitute

--The object of the invention is achieved by a first method which forms a first commutative checksum for digital data grouped into a number of data segments by a computer, forming a first segment checksum for each data segment, forming a first commutative checksum by a commutative operation ($\oplus$) on the first segment checksums, and cryptographically protecting the first commutative checksum using a cryptographic operation.

The object of the invention is also achieved with a second method which checks a predetermined cryptographic commutative checksum for digital data grouped into a number of data segments by a computer which has a predetermined

cryptographic checksum allocated to the digital data, and subjecting this cryptographic checksum to an inverse cryptographic operation to form a reconstructed first commutative checksum, forming a second segment checksum for each data segment, forming a second commutative checksum by a commutative operation on (⊕) the second segment checksums, and checking for a match between the second commutative checksum and the reconstructed first commutative checksum.

The object of the invention is also achieved with a third method which implements elements of both the first and second methods.

The object of the invention is also achieved with a first arrangement that forms a first commutative checksum for digital data grouped into a number of data segments which has an arithmetic and logic unit, a segment checksum that is formed for each data segment, a commutative operation that forms the first commutative checksum by operation on the segment checksums and a cryptographic operation that cryptographically protects the commutative checksum.

The object of the invention is also achieved with a second arrangement that checks a predetermined first commutative checksum allocated to digital data grouped into a number of data segments, that has an arithmetic and logic unit, an inverse cryptographic operation to form a first cryptographic checksum from a cryptographic commutative checksum formed by a cryptographic operation, a second segment checksum which is formed for each data segment, a commutative operation that operates on the second segment checksums which forms a second commutative checksum, and a comparator which checks for a match between the second commutative checksum and the first commutative checksum.

The object of the invention is also achieved with a third arrangement which implements elements of the first and second arrangements.--

On page 3, cancel lines 1 and 2.

in line 3, before "method", insert --first--, and cancel "according to Claim 1";

in line 9, before "method", insert --second--, and cancel "according to Claim 2";

in line 18, before "method", insert --third--, and cancel "according to Claim 3";

On page 4, in line 1, before "arrangement", insert --second--, and cancel "according to Claim 12", and cancel "exhibits" and substitute --has-- therefor;

in line 9, before "arrangement", insert --third--, and cancel "according to Claim 13", and cancel "exhibits" and substitute --has-- therefor;

On page 5, in line 2, cancel "the" and substitute --these-- therefor;

in line 3, cancel "the fact";

in line 5, after "received", insert --,--;

in line 7, before "checking", insert --data integrity--, and cancel "of the integrity of the data";

in line 9, cancel "Illustratively, the" and substitute --The-- therefor; and

in line 16, cancel "obtained from the dependent claims" and substitute --discussed below--.

On page 6, in line 1, cancel "so-called";

in line 17, cancel "," and substitute --in which-- therefor, and cancel "of which";

in line 25, cancel "Even if the" and substitute --The-- therefor;

in line 26, cancel "is"; and

in line 28, cancel ", this" and cancel "represent" and substitute --imply-- therefor.

On page 7, before line 1, insert

--**BRIEF DESCRIPTION OF THE DRAWINGS** -- ;

in line 1, cancel "The Figure shows" and substitute --The single Figure is a block diagram showing-- therefor, and cancel "," and substitute --in which-- therefore;

in line 2, after "segments", insert --are--;

above line 4, insert

--**DESCRIPTION OF THE PREFERRED EMBODIMENTS**--;

in line 7, after "data", insert --,--;

in line 8, cancel "it is of importance to ensure their integrity" and substitute --integrity must be maintained-- therefor;

in line 10, cancel "Both the" and substitute --The-- therefor;

in line 11, after "A2", insert --,--, and cancel "text" and substitute -- following text,-- therefor;

in line 12, cancel "which follows in each case" and substitute --each-- therefor;

in line 14, cancel "in the text which follows" and substitute --below-- therefor;

in line 19, cancel "[lacuna]" and substitute --formed-- therefor;

in line 20, cancel "checksum" and substitute --checksums-- therefor;

in line 22, cancel "[2]" and substitute --Kiyek & Schwarz-- therefor; and

in line 27, cancel "method" and substitute --operation-- therefor.

On page 8, in line 28, cancel "methods" and substitute --functions-- therefor;

On page 9, after "second", insert --segment--;

in line 4, after "further", insert --comparative--;

in line 15, cancel "and" and substitute --, possibly indicating-- therefor;

in line 16, cancel "is found and" and substitute --such a condition would-- therefor;

in line 20, cancel "so-called";

in line 24, after "first", insert --computer--;

in line 25, after "second", insert --computer--;

in line 30, cancel "In the text which follows" and substitute --The text below explains-- therefor; and

in line 31, cancel "will be explained".

On page 10, in line 12, before "independently", insert --either--, and cancel "However, the method for forming the checksum and the method for checking the checksum can also be" and substitute --or-- therefor;

in line 15, cancel "it is provided not to transmit digital data but" and substitute --the method also allows one-- therefor;

in line 16, cancel ", that is to say to store them" and substitute --by storing the digital data-- therefor;

in line 19, cancel "that is to say" and substitute --i.e.,-- therefor;

in line 25, cancel "Illustratively, the" and substitute --The-- therefor, and cancel "in that in the case of" and substitute --where-- therefor;

in line 26, cancel ",";

in line 27, cancel the first ",";

in line 32, cancel "take into consideration" and substitute --consider-- therefor; and

after line 33, insert --The above-described methods and arrangements are illustrative of the principles of the present invention. Numerous modifications and adaptions thereof will be readily apparent to those skilled in this art without departing from the spirit and scope of the present invention.--.

Cancel page 11.

IN THE CLAIMS:

On amended page 12, at line 1, cancel "New Patent Claims" and substitute **--I CLAIM AS MY INVENTION--** therefor;

Amend the following claims 1 through 3.

1. (Amended) A method [Method] for forming a first commutative checksum [(KP1)] for digital data comprising the steps of: [which are grouped into a number of data segments (Di, i = 1 .. n), by a computer,]

grouping said digital data into a number of data segments by a computer,

forming [a) in which] a first segment checksum [(PSi) is formed] for each said data segment [(Di)],

forming said [b) in which the] first commutative checksum [(KP1) is formed] by a commutative operation [(⊕)] on said [the] first segment checksums [(PSi)], and

cryptographically protecting said [c) in which the] first commutative checksum [(KP1) is cryptographically protected] by using a [at least one] cryptographic operation.

2. (Amended) A method [Method] for checking a predetermined cryptographic commutative checksum comprising the steps of: [which is allocated to digital data which are grouped into a number of data segments, by a computer,]

grouping digital data into a number of data segments by a computer,

allocating said predetermined cryptographic checksum to said digital data,

subjecting said [a) in which the] cryptographic commutative checksum

[is subjected] to an inverse cryptographic operation to form a first commutative [cryptographic] checksum [(KP1)],

forming [b) in which] a second segment checksum [(PSj) is formed] for each said data segment [(Dj, j = a .. z)],

forming [c) in which] a second commutative checksum [(KP2) is formed] by a commutative operation [(⊕)] on said [the] second segment checksums [(PSj)], and

checking said [d) in which the] second commutative checksum [(KP2) is checked] for a match with said [the] first commutative checksum [(KP1)].

3. (Amended) A method [Method] for forming and checking a first commutative checksum [(KP1)] for digital data comprising the steps of: [which are grouped into a number of data segments (Di, i = 1 .. n), by a computer,]

grouping said digital data into a number of data segments by a computer,

forming [a) in which] a first segment checksum [(PSi) is formed] for each said data segment [(Di)],

forming said [b)in which the] first commutative checksum [(KP1) is formed] by a commutative operation [(⊕)] on said first [the] segment checksums [(PSi)],

cryptographically protecting said [c) in which the] first commutative checksum [(KP1) is cryptographically protected] by using at least one cryptographic operation, which forms a cryptographic commutative checksum [being formed],

subjecting said [d) in which the] cryptographic commutative checksum [(KP1) is subjected] to an inverse cryptographic operation to form a reconstructed first [reconstructed] cryptographic checksum [(KP1)],

forming [e) in which] a second segment checksum [(PSj) is formed] for

each said data segment [(Dj, j = a .. z)] of said [the] digital data to which said [the] first commutative checksum [(KP1)] is allocated,

forming [f) in which] a second commutative checksum [(KP2) is formed] by a commutative operation [(⊕)] on said [the] second segment checksums [(PSj)], and

checking said [g) in which the] second commutative checksum [(KP2) is checked] for a match with said [the] reconstructed first [reconstructed] commutative checksum (KP1).

Cancel claim 4 and substitute the following claims 21, 22, and 23 therefor.

21. A method according to claim 1, further comprising the step of:

forming said first segment checksums in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

22. A method according to claim 2, further comprising the step of:

forming said second segment checksums in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

23. A method according to claim 3, further comprising the step of:

forming said first segment checksums and said second segment checksums in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

Cancel claims 5 and 6, and substitute the following claims 24, 25, and 26 therefor.

24. A method according to claim 1, wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

25. A method according to claim 2, wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

26. A method according to claim 3, wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Cancel claim 7 and substitute the following claims 27, 28, and 29 therefor.

27. A method according to claim 1, wherein:

said commutative operation exhibits the property of associativity.

28. A method according to claim 2, wherein:

said commutative operation exhibits the property of associativity.

29. A method according to claim 3, wherein:

said commutative operation exhibits the property of associativity.

Cancel claim 8 and substitute the following claims 30, 31, and 32 therefor.

30. A method according to claim 1, further comprising the step of:

protecting said digital data wherein said data segments have no ties to a specific ordering.

31. A method according to claim 2, further comprising the step of:

protecting said digital data wherein said data segments have no ties to a specific ordering.

32. A method according to claim 3, further comprising the step of:

protecting said digital data wherein said data segments have no ties to a specific ordering.

Cancel claim 9 and substitute the following claims 33, 34, and 35 therefor.

33. A method according to claim 1, further comprising the steps of:

protecting said digital data, and

processing said digital data in accordance with a network management protocol.

34. A method according to claim 2, further comprising the steps of:

protecting said digital data, and

processing said digital data in accordance with a network management protocol.

35. A method according to claim 3, further comprising the steps of:

protecting said digital data, and

processing said digital data in accordance with a network management protocol.

Amend the following claims 10 through 12.

10. (Amended) An arrangement [Arrangement] for forming a first commutative checksum [(KP1)] for digital data which are grouped into a number of data segments [(Di, i = 1 .. n)], said arrangement comprising:

[by means of] an arithmetic and logic unit, [which is arranged in such a manner that]

[a)] a first segment checksum, which [(PSi)] is formed for each said data segment [(Di)],

[b) the first commutative checksum (KP1) is formed by] a commutative operation [(⊕)] which forms said first commutative checksum by operating on said [the] segment checksums [(Psi)], and

[c) the first commutative checksum (KP1) is cryptographically protected by using at least one] a cryptographic operation which cryptographically protects said first commutative checksum.

11. (Amended) An arrangement [Arrangement] for checking a predetermined first commutative checksum which is allocated to digital data which are grouped into a number of data segments, said arrangement comprising:

[by means of] an arithmetic and logic unit, [which is arranged in such a manner that]

[a) the cryptographic commutative checksum is subjected to] an inverse cryptographic operation to form a first cryptographic checksum [(KP1)] from a

cryptographic commutative checksum formed by a cryptographic operation,

[b)] a second segment checksum [(Psj)] which is formed for each said data segment [(Dj, j = a .. z)],

[c) a second commutative checksum (KP2) is formed by] a commutative operation [(⊕)] which operates on said [the] second segment checksums [(PSj)] which forms a second commutative checksum, and

[d)] a comparator which checks for a match between said [the] second commutative checksum [(KP2) is checked for a match with the] and said first commutative checksum [(KP1)].

12. (Amended) An arrangement [Arrangement] for forming and checking a first commutative checksum [(KP1)] for digital data which is grouped into a number of data segments [(Di, i = 1 .. n)], said arrangement comprising:

[by means of] an arithmetic and logic unit, [which is arranged in such a manner that]

[a)] a first segment checksum, which [(PSi)] is formed for each said data segment [(Di)],

[b) the first commutative checksum (KP1) is formed by] a commutative operation [(⊕)] which forms said first commutative checksum by operating on said first [the] segment checksums [(Psi)],

[c) the first commutative checksum (KP1) is cryptographically protected by using at least one] a cryptographic operation which cryptographically protects said first commutative checksum, [a cryptographic commutative checksum being formed,]

a cryptographic commutative checksum formed by said cryptographic operation,

[d) the cryptographic commutative checksum is subjected to] an inverse cryptographic operation to form a first cryptographic checksum [(KP1)] from

said cryptographic commutative checksum,

[e)] a second segment checksum [(PSj)] which is formed for each said data segment [(Dj, j = a .. z)] of said [the] digital data to which said [the] first commutative checksum [(KP1)] is allocated,

[f) a second commutative checksum (KP2) is formed by] a commutative operation [(⊕)] which operates on said [the] second segment checksums [(Psj)] which forms a second commutative checksum, and

[g)] a comparator which checks for a match between said [the] second commutative checksum [(KP2) is checked for a match with the] and a reconstructed first [reconstructed] commutative checksum [(KP1)].

Cancel claim 13 and substitute the following claims 36, 37, and 38 therefor.

36. An arrangement according to claim 10, wherein:

said first segment checksums are formed in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

37. An arrangement according to claim 11, wherein:

said second segment checksums are both formed in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

38. An arrangement according to claim 12, wherein:

said first segment checksums and said second segment checksums are both formed in accordance with a type selected from the group consisting of a hashing value, a CRC code, and a cryptographic one-way function.

Cancel claims 14 and 15, and substitute the following claims 39, 40, and 41 therefor.

39. An arrangement according to claim 10 wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

40. An arrangement according to claim 11 wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

41. An arrangement according to claim 12 wherein:

said cryptographic operation is an operation selected from the group consisting of a symmetric cryptographic method and an asymmetric cryptographic method.

Cancel claim 16 and substitute the following claims 42, 43, and 44 therefor.

42. An arrangement according to claim 10 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

43. An arrangement according to claim 11 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

44. An arrangement according to claim 12 wherein said commutative operation exhibits the property of associativity via the arrangement of said arithmetic and logic unit.

Cancel claim 17 and substitute the following claims 45, 46, and 47 therefor.

45. An arrangement according to claim 10 wherein:
said digital data are protected, and
said data segments have no ties to a specific ordering.

46. An arrangement according to claim 11 wherein:
said digital data are protected, and
said data segments have no ties to a specific ordering.

47. An arrangement according to claim 12 wherein:
said digital data are protected, and
said data segments have no ties to a specific ordering.

Cancel claim 18 and substitute the following claims 48, 49, and 50 therefor.

48. An arrangement according to claim 10 wherein:
said digital data are protected via an arrangement of said arithmetic and logic unit, and
said digital data are processed in accordance with a network management protocol.

49. An arrangement according to claim 11 wherein:

said digital data are protected via an arrangement of said arithmetic and logic unit, and

said digital data are processed in accordance with a network management protocol.

50. An arrangement according to claim 12 wherein:

said digital data are protected via an arrangement of said arithmetic and logic unit, and

said digital data are processed in accordance with a network management protocol.

IN THE ABSTRACT:

On page 17, cancel lines 3-5;

in line 9, cancel "are specified. In the method," and substitute -- implement-- therefor; and

in line 10, cancel "is".

REMARKS:

The present Amendment revises the specification and claims to conform to United States patent practice, before examination of the present PCT application in the United States National Examination Phase. All of the changes are editorial and no new matter is added thereby.

The following changes are not intended to be a surrender of any of the subject matter of the claims:

- the amendment of claims 1, 2, 3, 10, 11, and 12
- the cancellation of claim 4, and the substitution of claims 21, 22, and 23 therefor
- the cancellation of claim 5 and 6, and the substitution of

claims 24, 25, and 26 therefor

- the cancellation of claim 7, and the substitution of claims 27, 28, and 29 therefor
- the cancellation of claim 8, and the substitution of claims 30, 31, and 32 therefor
- the cancellation of claim 9, and the substitution of claims 33, 34, and 35 therefor
- the cancellation of claim 13, and the substitution of claims 36, 37, and 38 therefor
- the cancellation of claims 14 and 15, and the substitution of claims 39, 40, and 41 therefor
- the cancellation of claim 16, and the substitution of claims 42, 43, and 44 therefor
- the cancellation of claim 17, and the substitution of claims 45, 46, and 47 therefor
- the cancellation of claim 18, and the substitution of claims 48, 49, and 50 therefor

Early examination on the merits is respectfully requested.

Submitted by,

Steven H. Noll (Reg. No. 28,982)

Steven H. Noll
Hill & Simpson
A Professional Corporation
85th Floor - Sears Tower
Chicago, Illinois 60606
(312)876-0200 Ext. 3899
Attorney for Applicant(s)

BOX PCT

IN THE UNITED STATES DESIGNATED/ELECTED OFFICE
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE
UNDER THE PATENT COOPERATION TREATY--CHAPTER II

APPLICANT(S):	Martina Hanck, et al
ATTORNEY DOCKET NO.:	P99,1784
INTERNATIONAL APPLICATION NO:	PCT/DE98/00563
INTERNATIONAL FILING DATE:	25 February 1998
INVENTION:	"METHOD AND SYSTEM FOR PRODUCING AND CHECKING A HASH TOTAL FOR DIGITAL DATA GROUPED IN SEVERAL DATA SEGMENTS"

Assistant Commissioner for Patents,
Washington D.C. 20231

REQUEST FOR APPROVAL OF DRAWING ADDITIONS

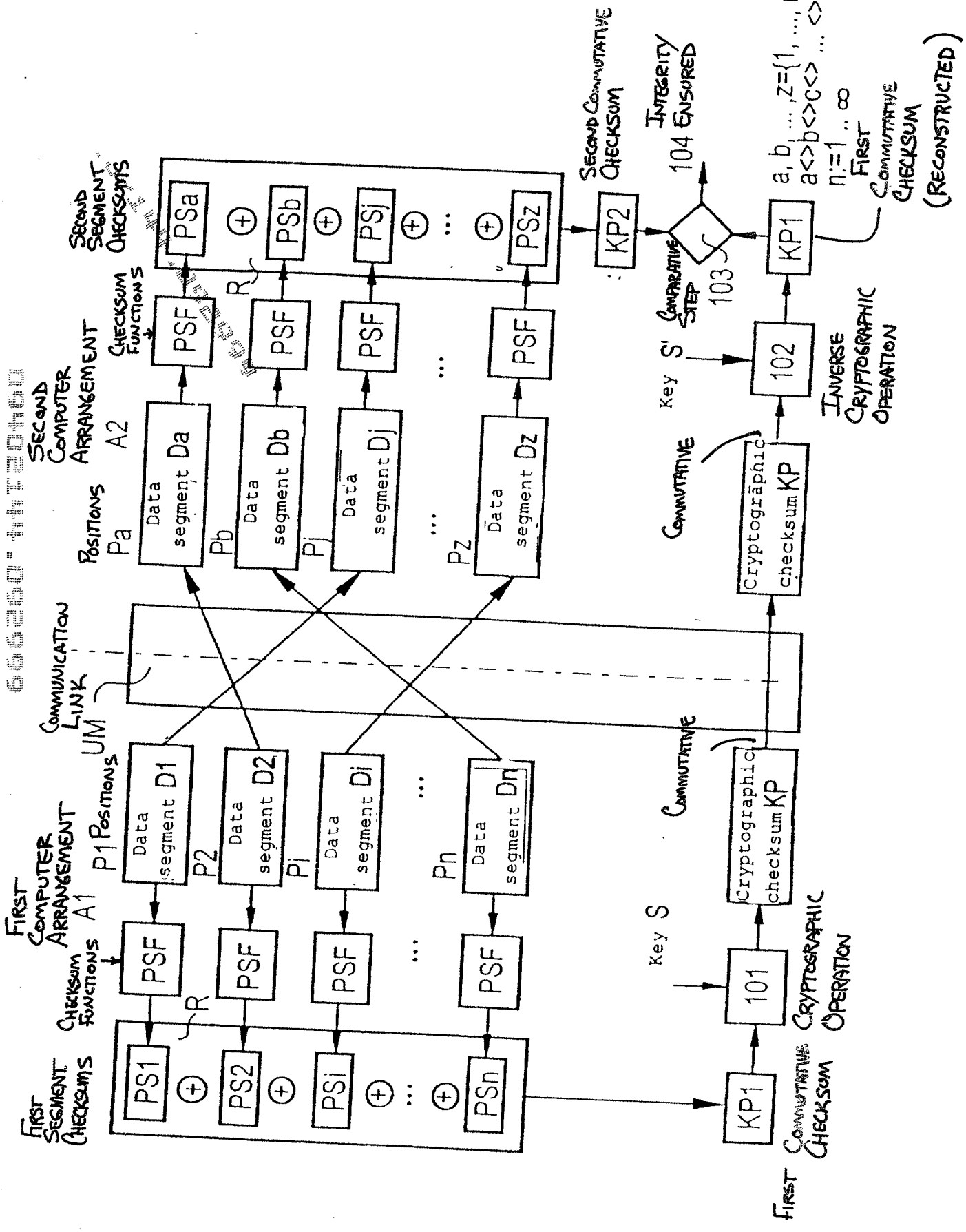
Sir:

Enclosed is a copy of the drawing (Single Figure), showing in red, the addition of labels to the elements depicted in the Single Figure. Approval of the additions to the Single Figure is respectfully requested.

Submitted by,

Steven H. Noll (Reg. No. 28,982)

Steven H. Noll
Hill & Simpson
A Professional Corporation
85th Floor - Sears Tower
Chicago, Illinois 60606
(312)876-0200 ext. 3899
Attorney for Applicant(s)


First Computer Arrangement A1
P1 Positions
Data segment D1
Data segment D2
Data segment Di
Data segment Dn
P2
Pi
Pn
UM
Communication Link
Positions Pa
Pb
Pj
Pz
Second Computer Arrangement A2
Data segment Da
Data segment Db
Data segment Dj
Data segment Dz
Checksum functions
PSF
R
First Segment Checksums
PS1
PS2
PSi
PSn
Second Segment Checksums
PSa
PSb
PSj
PSz
Key S
Key S'
101
102
Cryptographic checksum KP
Commutative Cryptographic Operation
Inverse Cryptographic Operation
Commutative
KP1
KP2
First Commutative Checksum
Second Commutative Checksum
Comparative Step
103
Integrity 104 Ensured
a, b, ..., z={1, ..., n}
a<>b<>c<> ... <>z
n:=1 .. ∞
(Reconstructed)

Description

Method and arrangement for forming and checking a checksum for digital data which are grouped into a number of data segments

In digital communications, i.e. during the exchange of digital data, it is frequently desirable to protect the transmission of the electronic data with respect to the most varied aspects.

A very significant aspect is the protection of the digital data to be transmitted against unauthorized modification, the so-called protection of the integrity of the data.

As a protection against unauthorized modification of digital data, the so-called cryptographic checksum, for example the digital signature, is known from [1]. The method described in [1] is based on forming a hashing value from the digital user data and the subsequent cryptographic processing of the hashing value by means of a cryptographic key. The result is a cryptographic checksum. To check the integrity, a corresponding cryptographic key is used for performing the inverse cryptographic operation on the checksum formed and the result is compared with the hashing value again calculated from the user data. The integrity of the user data is ensured when the hashing values are matched.

This previously customary procedure necessitates that the complete user data must be present on the receiver side in the identical order in which they were present when the hashing value was formed since otherwise the formation of the hashing value leads to an errored value. In digital communications, however, it is frequently customary to subdivide and to transmit the user data to be transmitted in relatively small data segments which are

also called data packets, due to protocol boundary conditions.

The data segments are frequently not tied to a defined order or it is not possible to guarantee a defined sequential arrival of the data segments. In the method from [1], it is therefore required for the complete user data to be reassembled again on the receiver side, that is to say after the transmission of the data segments, in the order in which they were originally sent. The data to be transmitted can only be verified in this order. However, this frequently means considerable additional expenditure for the flow control of the data segments inasmuch as this is possible at all within the framework of the protocol used.

From [2], commutative operations are known. In [2], a general definition for commutative operations is also specified. Illustratively, a commutative operation can be understood to be an operation in which the order of individual operations is unimportant and each order of individual operation always leads to the same total operation. A commutative operation can be, for example, an EXOR operation, an additive operation or also a multiplicative operation.

From [3], a method and a device for generating check code segments for the occurrence of source data and for determining errors in the source data are known.

The invention is thus based on the object of specifying methods and arrangements for forming and checking a first commutative checksum for digital data which are grouped into a number of data segments, in which a flow control for the individual data segments is no longer required.

The object is achieved by the method according to Claim 1, by the method according to Claim 2, by the method according to Claim 3, by the arrangement according to Claim

11, by the arrangement according to Claim 12 and by the arrangement according to Claim 13.

In the method according to Claim 1, a first segment checksum is formed for each data segment for digital data which are grouped into a number of data segments. The first segment checksums formed are combined by a commutative operation to form a first commutative checksum.

In the method according to Claim 2, a predetermined first commutative checksum, which is allocated to digital data which are grouped into a number of data segments, is checked. This is done by a second segment checksum being formed for each data segment and a second commutative checksum being formed by a commutative operation on the second segment checksum. The second commutative checksum and the first commutative checksum are checked for a match.

In the method according to Claim 3 for forming and checking a first commutative checksum for digital data which is grouped into data segments, a first segment checksum is formed for each data segment and the first data checksums are combined by a commutative operation to form a first commutative checksum. For each data segment of the digital data to which the first commutative checksum is allocated, second segment checksums are formed and a second commutative checksum is formed by commutative operation on the second segment checksums. The second commutative checksum and the first commutative checksum are checked for a match.

The arrangement according to Claim 11 exhibits an arithmetic and logic unit which is arranged in such a manner that a segment checksum is formed for each data segment and that the first commutative checksum is formed by a commutative operation on the segment checksums.

The arrangement according to Claim 12 exhibits an arithmetic and logic unit which is arranged in such a manner that a second segment checksum is formed for each data segment, a second commutative checksum is formed by a commutative operation on the second segment checksums, and the second commutative checksum (KP2) is checked for a match with the first commutative checksum (KP1).

The arrangement according to Claim 13 exhibits an arithmetic and logic unit which is arranged in such a manner that the following method steps are performed:

a) a segment checksum is formed for each data segment,

b) the first commutative checksum is formed by a commutative operation on the segment checksums,

c) a second segment checksum is formed for each data segment of the digital data to which the first commutative checksum is allocated,

d) a second commutative checksum is formed by a commutative operation on the second segment checksums, and

e) the second commutative checksum is checked for a match with the first commutative checksum.

A considerable advantage of the methods and of the arrangements can be seen in the fact that, by using a commutative operation for individual checksums of the data segments, a flow control for the order of the individual data segments is no longer required.

Furthermore, it is no longer required to reassemble the complete user data in the original order in which the first commutative checksums were formed. The order of the individual data segments is no longer of significance in the formation of the commutative checksum.

If the digital data are transmitted between two arrangements, a further advantage of the methods can be seen in the fact that the checking of the integrity can already be begun before all data segments have been received since it is no longer required to maintain the original order in forming the first checksum. This leads to a timesaving in the checking of the integrity of the data.

Illustratively, the invention can be seen in the fact that a checksum is formed in the case of a number of data segments which, together, form the data to be protected, and the individual checksums of the data segments are commutatively combined with one another.

Advantageous further developments of the invention are obtained from the dependent claims.

It is advantageous to protect the first commutative checksum cryptographically by using at least one cryptographic operation.

The result of this further development is that the cryptographic security of the data is considerably increased. A cryptographic operation in this sense is, for example, the encrypting of the first commutative checksum with a symmetric or also with an assymetric encryption method which forms a cryptographic checksum. On the receiver side, the inverse cryptographic method to the cryptographic method is performed in order to ensure cryptographic security.

To form a checksum within the context of the document, various possibilities are known:

- a checksum can be formed by forming hashing values for the individual data segments;

- the checksums can also be formed by so-called cyclic codes (Cyclic Redundancy Check, CRC);
- a cryptographic one-way function can also be used for forming the checksums for the data segments.

The methods can be advantageously used in various application scenarios.

The methods can be used both in the transmission of digital data for protection against manipulation of the data, and in the archiving of digital data in a computer in which the first commutative checksum is formed and stored together with the data to be archived. The first commutative checksum can be checked when the digital data are loaded from the archive memory in order to detect any manipulation of the archived data.

The method can be advantageously used for protecting digital data, the data segments of which are not tied to an order. Examples of such data segments are packet-oriented communication protocols, for example network management protocols such as the Simple Network Management Protocol (SNMP) or the Common Management Information Protocol (CMIP).

In the text which follows, an illustrative embodiment of the invention will be explained in greater detail with reference to a Figure. Even if the illustrative embodiment is explained with reference to the Simple Network Management Protocol (SNMP) in the text which follows, this does not represent any restriction on the applicability of the method. The method can be used whenever it is of importance to ensure integrity protection for digital data which are grouped into a number of data segments.

The Figure shows two arrangements, data segments being transmitted from the first arrangement to the second arrangement.

In the Figure, a first computer arrangement A1, in which data segments (Di, i = 1 .. n) are stored, is shown symbolically. The data segments Di together form the digital data which are also designated as user data, for which it is of importance to ensure their integrity.

Both the first computer arrangement A1 and a second computer arrangement A2 described in the text which follows in each case contain an arithmetic and logic unit R which is arranged in such a manner that the method steps described in the text which follows are performed.

In the first arrangement A1, the data segments Di are arranged at positions Pi within the total data stream. For each data segment Di, a first segment checksum PSi is [lacuna] by using a checksum function PSF. The individual first segment checksum PSi are combined to form a first commutative checksum KP1 by a commutative operation as defined and described in [2]. The commutative operation on the individual checksums PSi are shown symbolically by an EXOR symbol $\oplus$ in the Figure.

The first commutative checksum KP1 is subjected to a cryptographic method, a symmetric or asymmetric method, by using a first cryptographic key S (step 101). The result of the cryptographic operation is a cryptographic checksum KP.

Both the data segments Di and the cryptographic checksum KP are transmitted by a transmission medium, preferably a line or also a logical connection which is symbolically shown by a communication link UM in the Figure,

to a second arrangement A2 where they are received.

The crossing arrows of the data segments Di in the Figure indicate that, due to the transmission of the data segments Di, these are received in positions Pj (j = a .. z) which are displaced compared with the order in the first arrangement A1.

Thus, a data segment D2 at the first position P1 is received as data segment Da in the second arrangement A2. Data segment D1 is received as data segment Dc in the second arrangement. Data segment Dn is received as received data segment Db at the second position P2 in the second arrangement A2.

In accordance with the method used, either the first cryptographic key S is used for performing the inverse cryptographic operation on the cryptographic checksum KP if a symmetric encryption method is used, or a second cryptographic key S' is used if an asymmetric cryptographic method is used.

The result of the inverse cryptographic operation (step 102) is again the first commutative checksum KP1 with correct encryption and decryption.

This checksum is stored in the second arrangement A2. For the comparison of the data segments Dj, which are now received in permutated order compared with the original order during the formation of the first commutative checksum KP1, second segment checksums Psj are formed for the received data segments Dj, again using the same checksum methods PSF.

The resultant second checksums PSj are again commutatively combined with one another to form a second commutative checksum KP2.

In a further step 103, a check is made whether the first commutative checksum KP1 matches the second commutative checksum KP2.

If this is so, the integrity of the data segments Di, and thus the integrity of all the digital data, is ensured (step 104) if the cryptographic methods used or, respectively, the methods used for forming checksums ensure the corresponding cryptographic security.

If the first cryptographic checksum KP1 does not match the second cryptographic checksum KP2, the integrity of the data segments Di would be violated and a manipulation of the data is found and preferably reported to a user of the system.

The protocol data units (PDU) in SNMP are structured in such a manner that the user information (so-called variable bindings) can contain a list of objects (object indicators, OID/value pairs). The order of the objects within a PDU is not specified so that it is possible for a permutation of the objects to occur during the transmission of the PDUs between the first arrangement A1 and the second arrangement A2. The invention now makes it possible to form a single cryptographic checksum over all objects of an SNMP PDU without having to take into consideration the order of the objects or of the PDUs.

In the text which follows, alternatives to the illustrative embodiment described above will be explained.

The method for forming the checksum PSF can be, for example, a method for forming hashing values. However, methods for forming cyclic codes (Cyclic Redundancy Check, CRC) using feedback-type shift registers can also be used. In addition, cryptographic one-way functions can be used for forming the checksums PSi and, respectively, Psj.

Furthermore, the commutative operation can have the additional property of associativity.

Both the method for forming the checksum and the method for checking a checksum can be performed independently of one another. However, the method for forming the checksum and the method for checking the checksum can also be performed jointly.

Furthermore, it is provided not to transmit digital data but to archive the digital data, that is to say to store them in the first arrangement A1, together with the first commutative checksum KP1. When the archived data are reused, that is to say when the data segments Di are loaded from the memory of the first arrangement A1, the method for checking the first commutative checksum KP1 as described above will then be performed. The first arrangement A1 and the second arrangement A2 can thus be identical.

Illustratively, the invention can be seen in that in the case of a number of data segments which, together, represent the data to be protected, a checksum is formed for each data segment and the individual checksums of the data segments are commutatively combined with one another. This makes it possible to form and to check a checksum without having to take into consideration the order of the data segments.

In this document, the following publications have been quoted:

[1] W. Stallings, Sicherheit in Netzwerk und Internet (Security in Network and Internet), Prentice Hall, ISBN 3-930436-29-9, pp. 203-223, 1995

[2] K.-H. Kiyek and F. Schwarz, Mathmatik für Informatiker (Mathematics for Computer Scientists), Teubner Verlag, ISBN 3-519-03277-X, pp. 11-13, 1989

[3] DE-A 2 048 365

New Patent Claims

1. Method for forming a first commutative checksum (KP1) for digital data which are grouped into a number of data segments (Di, i = 1 .. n), by a computer,

a) in which a segment checksum (PSi) is formed for each data segment (Di),

b) in which the first commutative checksum (KP1) is formed by a commutative operation (⊕) on the segment checksums (PSi), and

c) in which the first commutative checksum (KP1) is cryptographically protected by using at least one cryptographic operation.

2. Method for checking a predetermined cryptographic commutative checksum which is allocated to digital data which are grouped into a number of data segments, by a computer,

a) in which the cryptographic commutative checksum is subjected to an inverse cryptographic operation to form a first cryptographic checksum (KP1),

b) in which a second segment checksum (PSj) is formed for each data segment (Dj, j = a .. z),

c) in which a second commutative checksum (KP2) is formed by a commutative operation (⊕) on the second segment checksums (PSj), and

d) in which the second commutative checksum (KP2) is checked for a match with the first commutative checksum (KP1).

3. Method for forming and checking a first commutative checksum (KP1) for digital data which are grouped into a number of data segments (Di, i = 1 .. n), by a computer,

a) in which a segment checksum (PSi) is formed for each data segment (Di),

Article 34 Amend't

b) in which the first commutative checksum (KP1) is formed by a commutative operation (⊕) on the segment checksums (PSi),

c) in which the first commutative checksum (KP1) is cryptographically protected by using at least one cryptographic operation, a cryptographic commutative checksum being formed,

d) in which the cryptgographic commutative checksum (KP1) is subjected to an inverse cryptographic operation to form a first reconstructed cryptographic checksum (KP1),

e) in which a second segment checksum (PSj) is formed for each data segment (Dj, j = a .. z) of the digital data to which the first commutative checksum (KP1) is allocated,

f) in which a second commutative checksum (KP2) is formed by a commutative operation (⊕) on the second segment checksums (PSj), and

g) in which the second commutative checksum (KP2) is checked for a match with the first reconstructed commutative checksum (KP1).

4. Method according to one of Claims 1 to 3, in which the segment checksums (PSi, PSj) are formed in accordance with at least one of the following types:

- forming a hashing value,
- forming CRC codes,
- using at least one cryptographic one-way function.

5. Method according to one of Claims 1 to 4, in which the cryptographic operation is a symmetric cryptographic method.

6. Method according to one of Claims 1 to 4, in which the cryptographic operation is an asymmetric cryptographic method.

Article 34 Amdt

7. Method according to one of Claims 1 to 6, in which the commutative operation (⊕) exhibits the property of associativity.

8. Method according to one of Claims 1 to 7, in which digital data are protected, the data segments (Di) of which are not tied to an order.

9. Method according to one of Claims 1 to 7, in which digital data are protected which are processed in accordance with a network management protocol.

10. Arrangement for forming a first commutative checksum (KP1) for digital data which are grouped into a number of data segments (Di, i = 1 .. n), by means of an arithmetic and logic unit which is arranged in such a manner that

a) a segment checksum (PSi) is formed for each data segment (Di), and

b) the first commutative checksum (KP1) is formed by a commutative operation (⊕) on the segment checksums (Psi), and

c) the first commutative checksum (KP1) is cryptographically protected by using at least one cryptographic operation.

11. Arrangement for checking a predetermined first commutative checksum which is allocated to digital data which are grouped into a number of data segments, by means of an arithmetic and logic unit which is arranged in such a manner that

a) the cryptographic commutative checksum is subjected to an inverse cryptographic operation to form a first cryptographic checksum (KP1),

b) a second segment checksum (Psj) is formed for each data segment (Dj, j = a .. z),

Article 34 Amdt

c) a second commutative checksum (KP2) is formed by a commutative operation (⊕) on the second segment checksums (PSj), and

d) the second commutative checksum (KP2) is checked for a match with the first commutative checksum (KP1).

12. Arrangement for forming and checking a first commutative checksum (KP1) for digital data which is grouped into a number of data segments (Di, i = 1 .. n), by means of at least one arithmetic and logic unit which is arranged in such a manner that

a) a segment checksum (PSi) is formed for each data segment (Di),

b) the first commutative checksum (KP1) is formed by a commutative operation (⊕) on the segment checksums (Psi),

c) the first commutative checksum (KP1) is cryptographically protected by using at least one cryptographic operation, a cryptographic commutative checksum being formed,

d) the crystographic commutative checksum (KP1) is subjected to an inverse cryptographic operation to form a first reconstructed cryptographic checksum (KP1),

e) a second segment checksum (PSj) is formed for each data segment (Dj, j = a .. z) of the digital data to which the first commutative checksum (KP1) is allocated,

f) a second commutative checksum (KP2) is formed by a commutative operation (⊕) on the second segment checksums (Psj), and

g) the second commutative checksum (KP2) is checked for a match with the first reconstructed commutative checksum (KP1).

13. Arrangement according to one of Claims 10 to 12,

Article 34 Amdt

in which the arithmetic and logic unit is arranged in such a manner that the segment checksums (PSi, PSj) are formed in accordance with at least one of the following types:

- forming a hashing value,
- forming CRC codes,
- using at least one cryptographic one-way function.

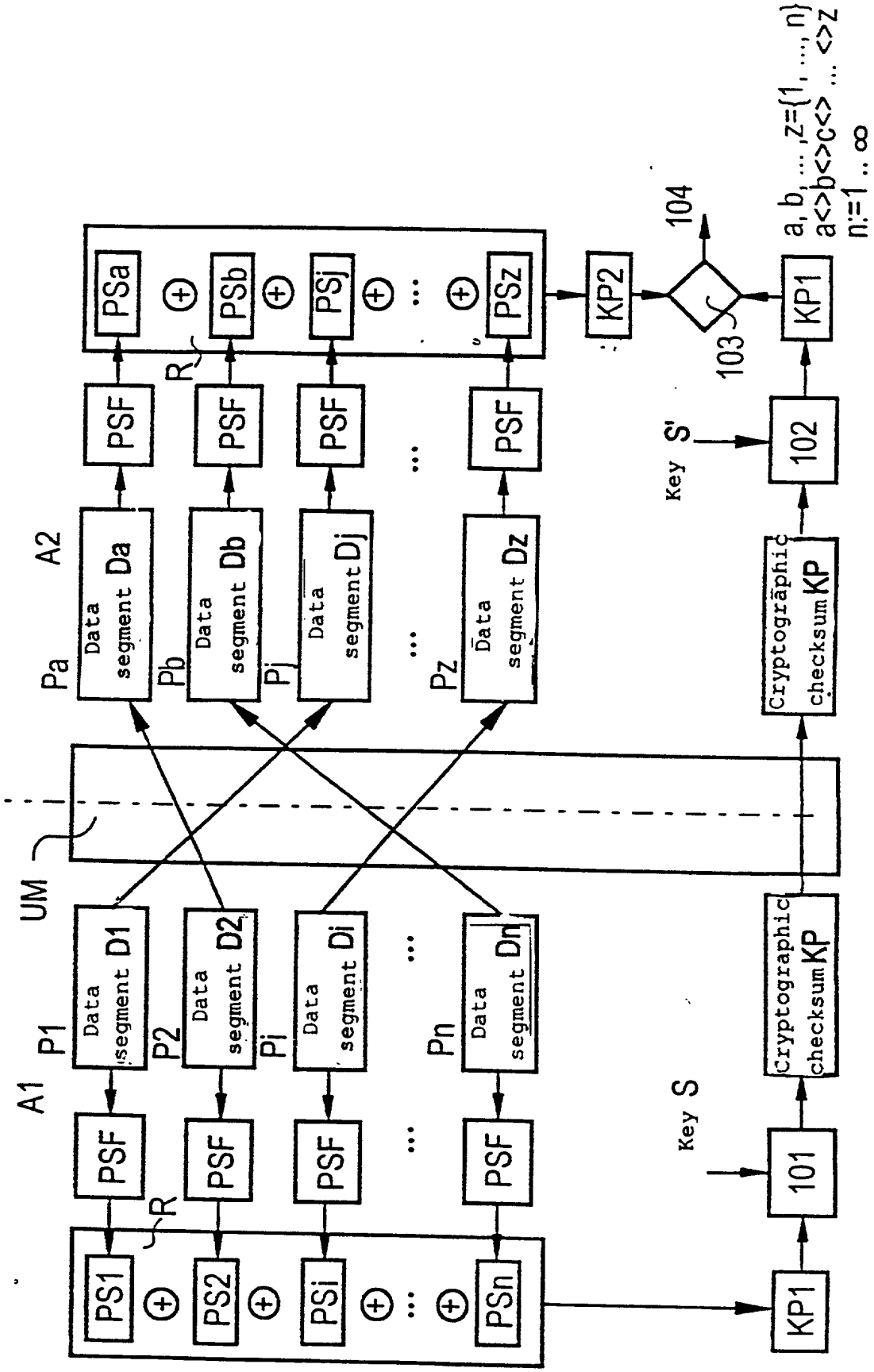
14. Arrangement according to one of Claims 10 to 13, in which the arithmetic and logic unit is arranged in such a manner that the cryptographic operation is a symmetric cryptographic method.

15. Arrangement according to one of Claims 10 to 13, in which the arithmetic and logic unit is arranged in such a manner that the cryptographic operation is an asymmetric cryptographic method.

16. Arrangement according to one of Claims 10 to 15, in which the arithmetic and logic unit is arranged in such a manner that the commutative operation ($\oplus$) exhibits the property of associativity.

17. Arrangement according to one of Claims 10 to 16, in which the arithmetic and logic unit is set up in such a manner that the digital data are protected, the data segments (Di) of which are not tied to an order.

18. Arrangement according to one of Claims 10 to 16, in which the arithmetic and logic unit is arranged in such a manner that the digital data are protected which are processed in accordance with a network management protocol.



Abstract

Method and arrangement for forming and checking a checksum for digital data which are grouped into a number of data segments

Methods and arrangements for forming a checksum and for checking a checksum for digital data which are grouped into a number of data segments are specified. In the method, a checksum is formed for each data segment. The individual checksums are combined to form a first commutative checksum by using a commutative operation. To check the first commutative checksum, a checksum is again formed for each data segment and the checksum is again combined to form a second commutative checksum under the method of a commutative operation. The first commutative checksum and the second commutative checksum are checked for a match.

Declaration and Power of Attorney For Patent Application
Erklärung Für Patentanmeldungen Mit Vollmacht
German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

Verfahren und Anordnung zur Bildung und Überprüfung einer Prüfsumme für digitale Daten, die in mehrere Datensegmente gruppiert sind

deren Beschreibung

(zutreffendes ankreuzen)

☒ hier beigefügt ist.

☐ am _____ als
PCT internationale Anmeldung
PCT Anmeldungsnummer _____
eingereicht wurde und am _____
abgeändert wurde (falls tatsächlich abgeändert).

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

_____
_____
_____
_____

the specification of which

(check one)

☐ is attached hereto.

☐ was filed on _____ as
PCT international application
PCT Application No. _____
and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Form PTO-FB-240 (8-83)
Patent and Trademark Office-U.S. DEPARTMENT OF COMMERCE

German Language Declaration

Prior foreign appplications
Priorität beansprucht

			Priority Claimed	
197 15 486.7	Germany	14. April 1997	☒	☐
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein
			☐	☐
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein
			☐	☐
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	Yes Ja	No Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozeßordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35. United States Code. §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occured between the filing date of the prior application and the national or PCT international filing date of this application.

(Application Serial No.) (Anmeldeseriennummer)	(Filing Date) (Anmeldedatum)	(Status) (patentiert, anhängig, aufgegeben)	(Status) (patented, pending, abandoned)
(Application Serial No.) (Anmeldeseriennummer)	(Filing Date) (Anmeldedatum)	(Status) (patentiert, anhängig, aufgeben)	(Status) (patented, pending, abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: *(Name und Registrationsnummer anführen)*

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

19-

And I hereby appoint

Messrs. John D. Simpson (Registration No. 19,842), Lewis T. Steadman (17,074), William C. Stueber (16,453), P. Phillips Connor (19,259), Dennis A. Gross (24,410), Marvin Moody (16,549), Steven H. Noll (28,982), Brett A. Valiquet (27,841), Thomas I. Ross (29,275), Kevin W. Guynn (29,927), Edward A. Lehmann (22,312), James D. Hobart (24,149), Robert M. Barrett (30,142), James Van Santen (16,584), J. Arthur Gross (13,615), Richard J. Schwarz (13,472) and Melvin A. Robinson (31,870), David R. Metzger (32,919), John R. Garrett (27,888) all members of the firm of Hill, Steadman & Simpson, A Professional Corporation.

Telefongespräche bitte richten an: *(Name und Telefonnummer)*

Direct Telephone Calls to: *(name and telephone number)*

312/876-0200
Ext. _____

Postanschrift:

Send Correspondence to:

HILL, STEADMAN & SIMPSON
A Professional Corporation
85th Floor Sears Tower, Chicago, Illinois 60606

Voller Name des einzigen oder ursprünglichen Erfinders: HANCK, Martina	Full name of sole or first inventor:
Unterschrift des Erfinders / Datum: X Martina Hanck X 03.02.98	Inventor's signature / Date
Wohnsitz: D-85635 Höhenkirchen, Germany DEX	Residence
Staatsangehörigkeit: Bundesrepublik Deutschland	Citizenship
Postanschrift: Am Grenzweg 2 D-85635 Höhenkirchen Bundesrepublik Deutschland	Post Office Addess
Voller Name des zweiten Miterfinders (falls zutreffend): HOFFMANN, Gerhard	Full name of second joint inventor, if any:
Unterschrift des Erfinders / Datum: X Gerhard Hoffmann X 03.02.98	Second Inventor's signature / Date
Wohnsitz: D-81547 München, Germany DEX	Residence
Staatsangehörigkeit: Bundesrepublik Deutschland	Citizenship
Postanschrift: Gozbertstr. 8/II D-81547 München Bundesrepublik Deutschland	Post Office Address

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).

Voller Name des dritten Miterfinders:	Full name of third joint inventor:
LUKAS, Klaus	
Unterschrift des Erfinders Datum	Inventor's signature Date
X Klaus Lukas X 03.02.98	
Wohnsitz	Residence
D-81739 München, Germany	
Staatsangehörigkeit	Citizenship
Bundesrepublik Deutschland	
Postanschrift	Post Office Address
Niemöllerallee 6	
D-81739 München Bundesrepublik Deutschland	

Voller Name des vierten Miterfinders (falls zutreffend):	Full name of fourth joint inventor, if any:
Unterschrift des Erfinders Datum	Inventor's signature Date
Wohnsitz	Residence
Staatsangehörigkeit	Citizenship
Postanschrift	Post Office Address

Voller Name des fünften Miterfinders (falls zutreffend):	Full name of fifth joint inventor, if any:
Unterschrift des Erfinders Datum	Inventor's signature Date
Wohnsitz	Residence
Staatsangehörigkeit	Citizenship
Postanschrift	Post Office Address

Voller Name des sechsten Miterfinders (falls zutreffend):	Full name of sixth joint inventor, if any:
Unterschrift des Erfinders Datum	Inventor's signature Date
Wohnsitz	Residence
Staatsangehörigkeit	Citizenship
Postanschrift	Post Office Address

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).